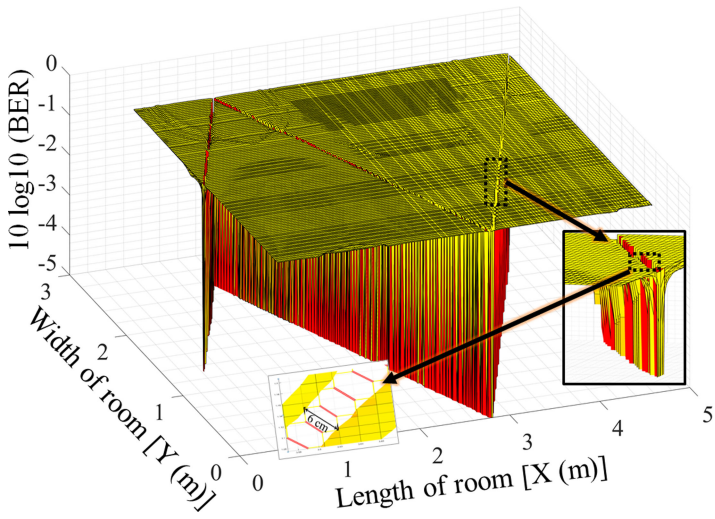
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Dynamic Physical-Layer Secured Link in a Mobile MIMO VLC System

Volume 12, Number 3, June 2020

Othman Isam Younus
Hoa Le Minh
Pham Tien Dat
Naokatsu Yamamoto
Anh T. Pham
Zabih Ghassemlooy



DOI: 10.1109/JPHOT.2020.2990798

IEEE photonics SOCIETY

IEEE

Dynamic Physical-Layer Secured Link in a Mobile MIMO VLC System

Othman Isam Younus [1], Hoa Le Minh [1], Pham Tien Dat [2], Naokatsu Yamamoto,[2] Anh T. Pham [3] and Zabih Ghassemlooy [1]

[1]Faculty of Engineering and Environment, Northumbria of University, Ellison Building, Newcastle Upon Tyne NE1 8ST, U.K.
[2]National Institute of Information and Communications Technology, Tokyo 184-8795, Japan
[3]Computer Communications Lab., The University of Aizu, Aizuwakamatsu 965-8580, Japan

DOI:10.1109/JPHOT.2020.2990798

Manuscript received February 24, 2020; revised April 9, 2020; accepted April 24, 2020. Date of publication April 27, 2020; date of current version May 26, 2020. The work of O. I. Younus was supported by the Northumbria University for his PhD study. Corresponding author: Othman Younus (e-mail: othman.younus@northumbria.ac.uk).

Abstract: This paper proposes a novel approach to provide a privately secured multiple-input and multiple-output visible light communication (VLC) in the mobility conditions. In the proposed system, a private secured VLC link is adaptively allocated to a mobile user all the time thanks to the movement tracking assistance by a camera-based detection system. The generation of the dynamic location-based scrambling matrix will be introduced providing a secured communication zone within a full normal coverage illumination area. An extensive range of numerical evaluation and practical experiments is carried out to demonstrate and evaluate the proposed system performance in different environment configurations including the mobility, camera resolutions, link range, and environment light intensity. We demonstrate that the proposed system is fully capable of securely steering the information with respect to a receiver location with a high level of reliability.

Index Terms: MIMO security, visible light communication, VLC, optical camera security, VLC security camera.

1. Introduction

With the advent of solid-state LED technological progress where the LED light can be modulated at high frequencies and the greatly increased demand for high-speed wireless data communication, the emerging VLC systems have been considered as one of the promising solutions for the future of wireless network generation [1] where the wireless carrier spectrum is increasingly higher. VLC will bring additional advantages alongside with the RF communication counterparts. Also, the integrated optics facilitate the usage of diffuse-lenses along with LEDs to obtain dual luminosity and communication in VLC systems, hence, reducing the carbon dioxide emissions by maintaining energy consumptions as low as possible [2]. The illumination intensity of LED lighting can be regulated based on the average current of the LED (DC-bias), binding it with data signal without affecting the beam profile of the LED light. VLC proves its validity to provide high data rate communication links in indoor environments, where the use of multiple-input-multiple-output (MIMO) VLC systems offers a Gbps data transmission [3]–[5]. As the light beam is concealed within the rooms or offices walls, VLC potentially offers secured communication in an enclosed space [6]. However, there is still a possibility for an eavesdropper to intercept the information within the

general illumination zone as a typical VLC system provides both illumination and communication in the same beam and coverage zone. Physical-layer security, therefore, is an ingenious technique offering an effective and strong encryption method to reduce an extra computation at upper layers since it can exploit the characteristics of the physical channels to secure the information from eavesdroppers by blocking the hacker from accessing the meaningful physical data [7]. It also eliminates the dependency of an encryption key at the receiver as highlighted in [8–11], where a keyless scheme was suggested to secure a VLC channel based on the wiretap channel estimation or the physical location of the receivers. MIMO based security system has been firstly proposed in [8], where we proposed a method to steer dedicated data to a receiving coverage area by utilizing the MIMO structure. Under this technique, data can be unlocked if a user is moving to a fixed area. In [9], [11] a static-secured multiple-input, single-output (MISO) VLC channel is proposed based on the physical layer, whereas [10] focused on combining the real-valued channel-state information (CSI) with chaotic sequences to further improve the physical layer security of the VLC system. In [12], a secure coding scheme based on polar codes was proposed for SISO and MISO VLC to achieve physical-layer security for indoor VLC systems under Wyner's wiretap model, which ensures that the wiretap channel is not affected with respect to the main channel.

In real-life applications, a user is usually in motion from time to time therefore to achieve the physical security, it is required that the system either to provide a greater security area or to track the user position to reallocate a secure coverage for the secured VLC link. The provision of a greater area leads to the fact that there is a problem to allocate more users as well as the security might be compromised since a hacker can move its receiver next to the legitimate user. The use of the tracking system requires the transmitter to update the user location regularly, either received by the uplink feedback from the user or it needs to self-detect the user location.

Obtaining a current position feedback from the receiver using the VLC uplink imposes a crucial challenge as (i) the induced irradiance of a narrow beam-width light source needs to be oriented to a fixed direction toward the receiver in the ceiling, (ii) energy limitation factor is restricting the usage of the LED to transmit information for the uplink channel, (iii) the light glare of the uplink might interfere with the downlink channel in regards to full-duplex communication producing a hindrance to human eyes in an indoor environment [13], and (iv) it might not be practical to have a VLC uplink due to the aesthetic point of view. Alternatively, techniques for self-determination of user location can be implemented to estimate the receiver position from the transmitter side.

In this paper, we propose a method to enhance the dynamic security of the physical layer in a MIMO VLC system using the optical tracking system. The proposed scheme provides a secure dynamic zone, which follows the receiver's position inside the illuminated zone compared with a static secured zone adopted in [8]. In addition, it differs from [9], where the secure link was proposed when the eavesdropper was expected to exist within a specified area, and [10], where the enhancement of the physical layer was deployed based on DCO-OFDM VLC. In [11] both transmit beamforming and jamming techniques were adopted to enhance communications secrecy for MISO VLC under multiple eavesdropping environment, thus requiring a trade-off between the beam profile and the minimum area with security.

By self-allocating a private physical communication channel for a user on the move, where the user position will be tracked in the transmitter side and correspondingly form an adaptive channel matrix unique to the user. Here we generate a varied scrambling matrix with respect to the unique receiver position, to form an exclusive data-recoverable zone within the original illumination area to prevent unauthorized access from receiving the original data. The main original contributions presented in this work will include (i) the development of a novel mathematical model to create a dynamic secure zone that is varied based on the receiver position within the illuminated region of a non-imaging MIMO system, (ii) the design of camera-based surveillance system integrated to the MIMO VLC transmitter to obtain self-determination of the VLC user/receiver position with different resolutions, distance and illumination conditions, and (iii) the customised utilization of image-processing techniques to obtain a high accuracy VLC user positioning system.

The paper is organized as follows. Section 2 presents the theory section of the VLC MIMO system and the followed algorithms to secure the channel. It also covers the image-processing

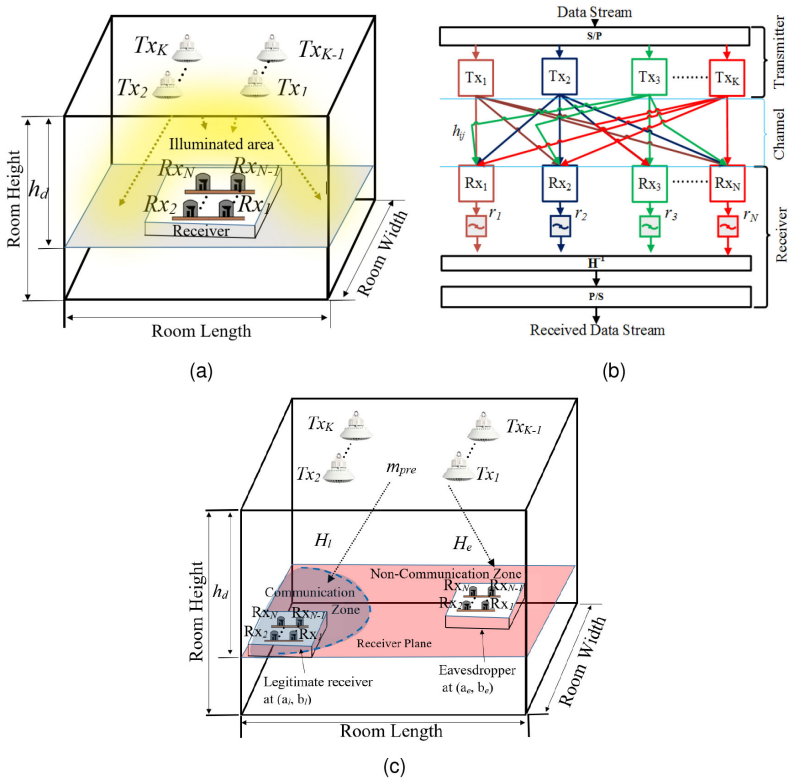


Fig. 1. (a) A standard schematic diagram of $K \times N$ non-imaging MIMO VLC system. (b) A typical block diagram for a $K \times N$ MIMO VLC. (c) A static secured MIMO VLC system [8].

techniques to define the dynamic communication zone for the MIMO system. System operation and results are outlined in Sections 3 and 4 respectively, followed by the conclusion and future work discussion in Section 5.

2. Physical Security for a MIMO VLC System

2.1 MIMO VLC Modelling

In a typical MIMO system, as shown in Fig. 1(a), there are K LED-based transmitters (or illumination sources, equivalently) placed symmetrically to provide flat-level illumination as well as wireless data communication. At each user, an N number of photodetector (PD) receivers is located to receive and recover transmitted data streams. The use of non-imaging MIMO VLC system offer a wide field-of-view and a high optical gain compared with imaging MIMO receivers [14], [15].

The transmitters send independent data streams continuously, and the number of transmitters and receivers can be varied depending on the requirement of the illumination footprint without affecting the principle of MIMO systems. However, the number of receivers should be equal to or larger than the number of transmitters i.e. $K \geq N$ [2], [16]. This condition is required to ensure the channel matrix is full rank.

A data stream is split into K parallel sources to intensity modulate K-LED groups as shown in Fig. 1(b). The emitted optical signal is defined as $\boldsymbol{m}_i$, where i is $1, \ldots, K$. The channel coefficient h_{ij} is the one from i^{th} LED (of the transmitter) to j^{th} PD (of a user). Before the data transmission, the MIMO system needs to estimate the channel coefficients for each pair of transmitter and receiver. The coefficients, i.e. the channel gain for each Tx-Rx path link, can usually be estimated using a pilot signal scheme. At the receiver, data can be recorded as:

$$\boldsymbol{r} = \mathbf{H}\boldsymbol{m} + \boldsymbol{n}, \tag{1}$$

where $\boldsymbol{m}$ represents the transmitted signal vector, $\boldsymbol{n}$ is the column vector of the noise for each link, and $\mathbf{H}$ denotes the user channel matrix which consists all DC gain coefficients from the i-th LED (of the transmitter) to j-th PD. Equation (1) can be further extended as follows:

$$\begin{bmatrix} r_1 \\ r_2 \\ . \\ . \\ r_K \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & . & h_{1K} \\ h_{21} & h_{22} & . & h_{2K} \\ . & . & . & . \\ . & . & . & . \\ h_{K1} & h_{K2} & . & h_{KK} \end{bmatrix} \cdot \begin{bmatrix} m_1 \\ m_2 \\ . \\ . \\ m_K \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ . \\ . \\ n_K \end{bmatrix}. \tag{2}$$

MIMO VLC link channels are typically line-of-sight (LOS), thus, a h_{ij} represents the DC channel gain is given by:

$$h_{ij} = I \frac{(m_l + 1)}{2\pi} \frac{A_{det}}{d_{ij}^2} \cos^{m_l}(\Phi_{ij}) \cos(\psi_{ij}) g(\psi_{ij}), \tag{3}$$

where I is the total luminous flux intensity of the source, m_l is the Lambertian radiation order (given by $m_l = \frac{-\ln(2)}{\ln(\cos(\Phi_{1/2}))}$), and the angle of irradiance is Φ_{ij}, ψ_{ij} is the angle of incidence, $g(\psi_{ij})$ is the optical concentrator gain, and d_{ij} is one form of the distance between Txj (LED of the transmitter) and Rxi (PD surface of the receiver).

There are different techniques to recover the data of a MIMO VLC system, however, zero-forcing (ZF) equaliser offers the lowest complexity to minimize the ISI as well as a linear phase in the transmission link with flat frequency response for the received signal [17]. The diversity in communications systems (i.e., VLC with MIMO in this case), which is adopted to improve the system performance (i.e., transmission capacity, link availability, etc.), depends on several factors including the field of view [2], type of receivers, i.e., non-imaging or imaging [14], the type of diversity schemes such as angle diversity [15] and maximal ratio combining (MRC). By knowing the full CSI from sending a pilot signal (PS), or in this case the channel matrix $\mathbf{H}$, the VLC receiver is able to fully recover the transmitted data where the received signal m_{rec} is given by:

$$\boldsymbol{m}_{\mathbf{rec}} = \mathbf{H}^{-1} \boldsymbol{r}. \tag{4}$$

2.2 Physical Security MIMO VLC - Static Scenario

Physical layer security based on the location in VLC provides a good measure to prevent hackers from accessing the meaningful signals due to the uniqueness of the location in the space domain. It provides a private link for a specific (or fixed) region inside the illuminated area for communication [8]. The use of position matrix is adopted to obtain a private link where the position matrix $\mathbf{P}$ is used to scramble the transmitted signal $\boldsymbol{m}$ which produces a pre-coded signal as:

$$\boldsymbol{m}_{\mathbf{pre}} = \mathbf{P}\, \boldsymbol{m}. \tag{5}$$

For two receivers placed at two different positions in the receiving plane, as shown in Fig. 1(c), the received signals for legitimate receiver $\boldsymbol{r}_l$ and eavesdropper $\boldsymbol{r}_e$ are given as:

$$\boldsymbol{r}_l = \mathbf{H}_l\, \boldsymbol{m}_{\mathbf{pre}} + \boldsymbol{n} = \mathbf{H}_l\, \mathbf{P}\, \boldsymbol{m} + \boldsymbol{n}, \tag{6}$$

$$\boldsymbol{r}_e = \mathbf{H}_e\, \boldsymbol{m}_{\mathbf{pre}} + \boldsymbol{n} = \mathbf{H}_e\, \mathbf{P}\, \boldsymbol{m} + \boldsymbol{n}, \tag{7}$$

where $\mathbf{H}_l$, $\mathbf{H}_e$ are the user channel gain matrices between transmitter and both legitimate and eavesdropper receivers as shown in Fig. 1, respectively. In order to define a secure zone for communication at the illuminated location (a_l, b_l) for the authenticated receiver, we have utilised a reference matrix $\mathbf{H}_p$, which is generated by considering the estimated channel gain at (a_0, b_0), is used for two reasons (i) should be given in advance to improve the transmit power constraint.; and (ii) security enhancement by limiting the width of the recoverable covered area. Note that, even if the eavesdropper has the knowledge of $\mathbf{H}_p$, meaningful data cannot be recovered and $\mathbf{H}_p$ represents

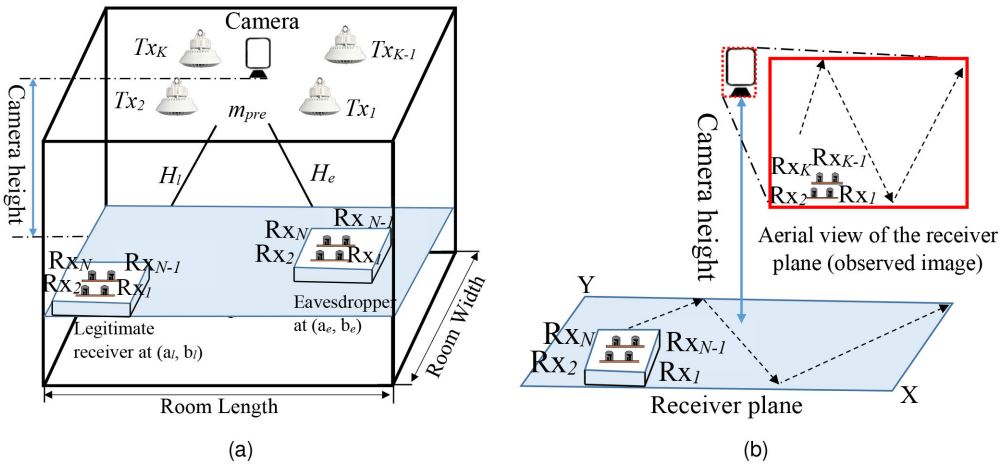


Fig. 2. (a) A camera-based system with $K \times N$ non-imaging MIMO system. (b) An optical tracking system deployment at the transmitter side.

another layer of security to allow a hybrid system where another gain is needed to achieve optimal security. Therefore, the scrambling matrix **P** is designed as:

$$\mathbf{P} = \mathbf{H}_l{}^{-1}\mathbf{H}_p. \tag{8}$$

Consequently, we have,

$$r_l = \mathbf{H}_l\,\mathbf{H}_l{}^{-1}\,\mathbf{H}_p\,m + n = \mathbf{H}_p\,m + n, \tag{9}$$

$$r_e = \mathbf{H}_e\,\mathbf{H}_l{}^{-1}\mathbf{H}_p\,m + n = \mathbf{H}_e\,\mathbf{H}_l{}^{-1}\mathbf{H}_p\,m + n. \tag{10}$$

In the transmitter side, the channel matrix of the legitimate receiver $\mathbf{H}_l$ is defined based on the coordinates of (a_l, b_l), given that the data cannot be recovered without the existence of the receiver inside the dedicated zone $\mathbf{H}_l$. In [8] the $\mathbf{H}_l$ is known in the transmitter side, hence, the user should move into the zone where the channel matrix is similar to $\mathbf{H}_l$ to allow the receiver to retrieve the data correctly. If the user is on the move, the system requires the user to update either its location or the transmitter should independently detect the user position. In the first approach, it is challenging due to the requirement of the uplink as mentioned above. In addition, the uplink can possibly be intercepted by an eavesdropper hence it is not totally safe.

2.3 Proposed Dynamic Secured MIMO VLC System

The provision of a private link for a specific region introduced in the [8] limits the user mobility as the secured channel is fixed. When a user is on the move, the system is required to be adaptive to change the steering direction to maintain the secured connectivity. Hence, the transmitter should be updated with the user location to ensure the free movement of the receiver without a need of updating its location periodically to the transmitter to maintain a secured link, we implement an optical tracking system with the aid of camera and image processing deployed at the transmitter side, hence, following the receiver position. This enables the transmitter to generate a dynamically dedicated secured communication zone that is private and unique for a user when it is on the move. Figure 2(a) shows a schematic diagram of a camera-based system placed in the middle of K LED-based transmitters.

Initially, a **P**-matrix is generated in the transmitter side based on the user-location information detected by the camera, as it is described in the subsequent section. **P** is then merged with the input data binary stream to produce the pre-coded data prior to splitting it in a parallel way to be transmitted incoherently via intensity modulation and direct detection (IM/DD). The receiver, on the other hand, includes N PDs to receive light and concurrently working out the channel matrix

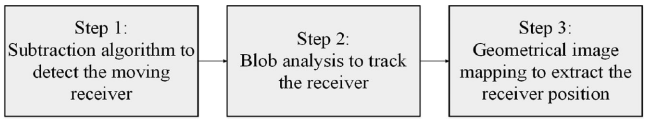


Fig. 3. Camera-based optical tracking system key steps.

to recover the original data, where each receiver's PD retrieves the linear combinations of all m_j links of data streams. Followed by obtaining the CSI-matrix between each pair Tx_i and Rx_j, a ZF equaliser is used to eliminate the channel's effect allowing the receiving of the authenticated data.

2.4 Optical Tracking System to Locate the User Position

By deploying a camera-based tracking system placed in the middle of the ceiling, the system can detect and track the location of the receiver as shown in Fig. 2(b), where the captured scene presents the position of the receiver within the illuminated region. The proposed camera operation process as shown in Fig. 3 includes three key steps:

- *Step 1: Object detection using a background subtraction algorithm based on Gaussian mixture models*

To locate the receiver position within the acquired data frames, initially, we proposed a background subtraction technique, which is a common approach used in order to detect moving objects using stationary cameras [18]. It can detect the moving receiver by comparing the differences between the real-time frame and the reference frame (without any other motion inside the frame). It is embedded by the deployment of the Mixture of Gaussians (MOG), a multi-modal background adaptive method to detect the foreground [18], to allow the system to accommodate the continuous changes in the illumination levels and temporal background clutter as addressed in [19]. We first convert the 1st frame of the RGB scene to the grayscale level (for simplicity sake, the grayscale intensity level of the RGB frame instead of the RGB frame is considered for the MOG analysis), the values of each pixel over time (i.e. the history of the information about assigned pixel) $\{x', y'\}$, is defined as:

$$\{M_1, ..M_t\} = \left\{ I_s \left(x,' y,' z\right) : 1 \leq z \leq t \right\}, \tag{11}$$

where I_s is the image sequence. The recent history of each pixel,$\{M_1, ..M_t\}$, is modelled by a mixture of G Gaussian distributions. The probability of observing the present pixel is used to identify the moving pixel measured by:

$$P\left(M_t\right) = \sum_{z=1}^{G} \omega_{z,t}\, \eta\left(M_t, \mu_{z,t}, \sigma_{z,t}^2\right), \tag{12}$$

where G is the number of distributions, the weight estimation (what segment of the information considered by this Gaussian) of the z^{th} Gaussian in the mixture at time t, and the mean value are $\omega_{z,t}$, $\mu_{z,t}$, respectively. η is the probability density function, the deviation around the average value is $\sigma_{z,t}$ [20]. Therefore, the distribution of these identified values of each pixel in the image plane is represented by the Gaussians mixture, henceforth the coming pixel, either to be characterized by one of the leading components of the model or, to considered as a foreground prior to updating the model [21].

These operations have applied to obtain the receiver, where the 1st frame is to initiate the MOG process, subsequently, to read the coming frame in order to define the history of pixel as highlighted in (11), hence, estimate the location of the receiver (foreground detection) using (12) as given in Fig. 4.

- *Step 2: Object tracking using Blob Analysis*

Blob analysis is a fundamental technique in vision analysis, in which a blob is defined as a region of connected pixels to track them [22]. It usually exploits the statistical information or the

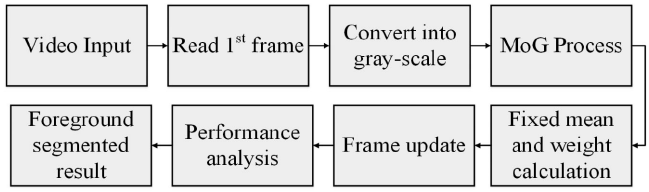


Fig. 4. Block diagram of Background subtraction.

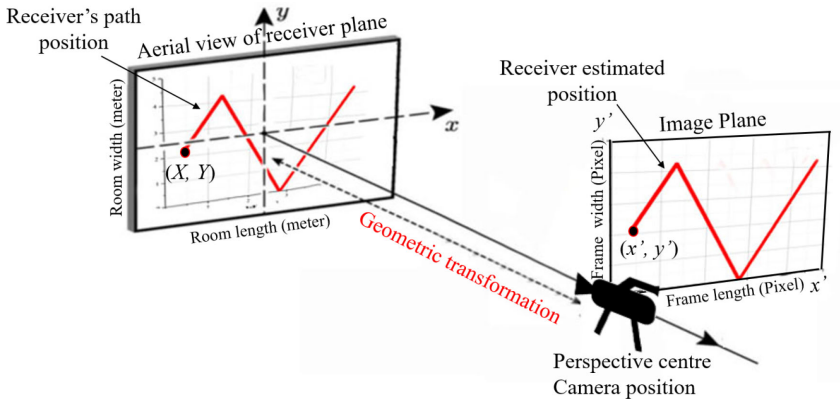


Fig. 5. Geometrical transformation between the image plane and the room dimensions.

spatial characteristics of blobs that satisfy certain criteria including the area, circumference, Feret diameter, blob shape, eccentricity rate in the frame, and the location [23]. The proposed system characterised the blob shape of the receiver as a bounding box (a rectangle shape that contains the receiver blob).

- *Geometrical transformation*

The presentation of the projection between the image plane and the room dimensions according to [24] generally includes the linear transformation, rotation, deviation, and the scaling prior to rescaling it to the physical units with the addition of the offsets if any exist. It estimates the position of legitimate receiver in the room-scale through mapping the position of tracked receiver in pixels to the coordinates of the room in the meter, as shows in Fig. 5. The conversion scale is:

$$X = (x' \times \text{Room}_{\text{length}}) \div \text{Frame length}, \tag{13}$$

$$Y = (y' \times \text{Room}_{\text{width}}) \div \text{Frame width}, \tag{14}$$

where X and Y are the estimated room dimensions coordinates, (x, y) are the receiver position in the image.

3. Experimental Demonstration

3.1 Experimental Setup

The proposed system in the previous section (2.3) is deployed, and the system block diagram is presented in Fig. 6. The experimental section covers the realisation of the moving receiver, where a tracking video is introduced based on the movement of the authenticated receiver. Initially, the VLC system is simulated using MATLAB and the number of receivers and the number of transmitters are assumed to be equal for the sake of simplicity, where $N = K = 4$. The positioning matrix is designed for each user's new position, hence precoding the input signal, which is non-return-to-zero on-off-keying (NRZ-OOK) data, as proposed in equation (5). Additionally, the transmitting simulation process was performed by taking a real LED impulse response measured for each transmitter.

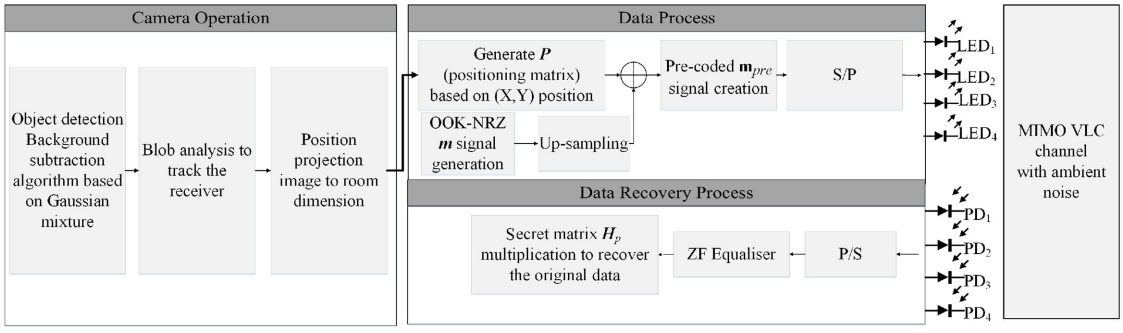


Fig. 6. Block diagram of the proposed system.

TABLE 1
VLC System Parameters

Room dimension	
Length(m)×width(m)×height(m)	5×3×3
Parameters	**Values**
Number of LED-based transmitters	4
Transmitters locations	$(1.25, 1.25)$,$(1.25, 3.75)$ $(3.75, 1.25)$,$(3.75, 3.75)$
LED Type	SR-01-WC310
Beam angle-based transmitter	$120°$
Number of sample (n)	10
LED Bandwidth	3 MHz
Data rate (R_B)	5 Mbit/sec
Transmitter gain	20 dB
Number of LED-based receivers	4
Receiver moving speed	0.53 m/s
Receiver dimension	10 cm × 10 cm
PD active area	15 mm^2
PD responsivity	0.6
PD field of view (FOV)	$180°$
Receiver sensitivity (used with AD8015 transimpedance amplifier)	-30 dBm
LPF cut-off frequency	$0.7 * R_B$
X-Y sweep resolution	1 cm × 1 cm
Noise parameters	
Equivalent noise bandwidth	R_B Hz
Background Current	500×10^{-6} A
Noise bandwidth factors($I2$, $I3$)	$0:562$; $0:0868$
Absolute temperature	313 kelvins degree
FET channel noise factor	1.5
FET transconductance	30×10^{-3} mS

The NRZ transmitted signal consists of 1000 bits length. Also, the ambient noise of an indoor environment is included in the channel where an additive white Gaussian noise is considered as represented in [17]. The key parameters of the VLC system are given in Table 1.

Subsequently, the receiver movement within the illuminated region is evaluated using a pre-designed equivalent-receiving plane (explained in the next section), hence, the motion path of the user is depicted in Fig. 7. The tracking video was then processed in MATLAB where the optical tracing including the subtraction algorithm, and the blob analysis is applied to extract the positions of receiver in the image plane (or screen) where the area of the receiver is set initially in Pixel units highlighted in Table 2, and hence being equivalently mapped into the room-scale. The optical tracking system parameters are outlined in Table 2.

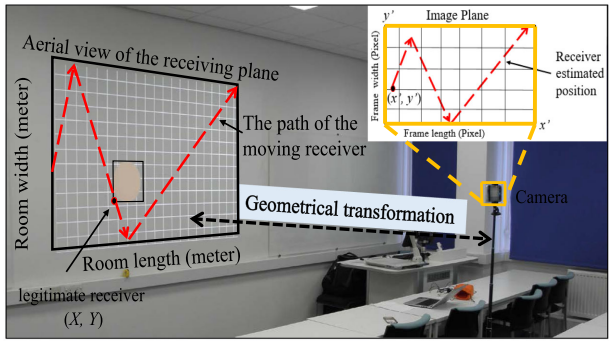


Fig. 7. Experiment set-up.

TABLE 2
Optical Tracking System Parameters

Parameters	Values
Camera sensor	12 MP CMOS
Focal length	4.2 mm (26 mm eff)
Pixel size	1.4 μm
Max aperture	F/1.7
Resolution	320×240, 640×480, 720×576, 1280×720
Frame rates	25 Fps
Measured ambient level(lux)	2 LUX (No light),
(Note: ISO office standard)	275 LUX (Low light),
	450 LUX (Indoor normal light)
Camera height (h)(i.e. distance between camera and receiver plane)	2 m, 3 m
Camera location	(2.5,2.5)
Camera field of view (FOV)	$90°$, $67.3°$
Number of Gaussian modes (used in the MOG model)	3
Number of initialisation frames (used in MOG model)	50 frames
Minimum blob area for 320×240	500 pixels
Minimum blob area for other resolutions	2000 pixels

3.2 Implementation Strategy

The process of camera position self-determination to locate the authenticated receiver, within its receiving field of view, and the encryption process is presented in Fig. 5. Likewise, a projection has been used to display (or mimic) a moving user on the screen, which is equivalent to a user moving on a room's floor in the set-up of Fig. 2(b). The camera is to monitor an equivalent-receiving plane (in MIMO VLC system) with different link distances, camera resolutions, and various illumination levels of the environment as given in Table 2.

For the sake of simplicity and to avoid the usage of the perspective transformation, the camera is positioned in the projected centre of the screen (i.e. room floor equivalently) from a distance *h* to form a collinear photogrammetric measurement (an object point and its photo image all lie along a straight line) between the receiver plane and the camera frame as depicted in Fig. 7.

The mapping from the screen/camera setup to the MIMO VLC system is shown in Fig. 5. The conversion scale is obtained through the utilisation of equations (13) and (14). Correspondingly, the image plane displays an aerial view of the designed scene and the illuminated region in the room, where the receiver positions and moving route are detected to facilitate the evaluation between the actual and estimated location of the legitimate receiver.

The room is normally lit by other artificial fluorescent lamps at 400 Lux level. The receiver is then able to recover the transmitted signal at the designed communication zone as in equation (9), whereas, at other positions outside this zone, data recovery is not feasible.

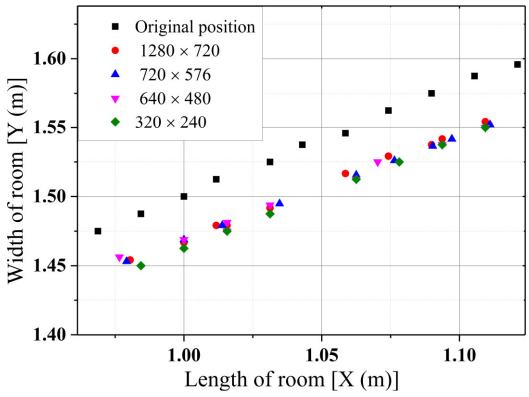


Fig. 8. Zoom in evaluation of the receiver tracking position for different camera resolutions (distance = 2 m, lux = 0).

TABLE 3
Tracking System Performance With Different Resolutions

Resolutions	Error Mean X(cm),Y(cm)	Standard Deviation X(cm),Y(cm)	Maximum Error X(cm),Y(cm)
1280×720	$2.44, 2.28$	$1.86, 2.07$	$15.23, 7.92$
720×576	$2.44, 2.25$	$1.81, 2.06$	$14.63, 7.81$
640×480	$2.52, 2.24$	$2.16, 2.06$	$19.53, 7.92$
320×240	$2.53, 2.14$	$2.73, 1.87$	$37.89, 7.92$

The system performance is investigated by performing different tests using various camera resolutions, transmission link including the camera, and multiple-level light conditions for each position of the receiver. BER vs SNR curve for the legitimate and eavesdropper receiver positions in the illuminated region were obtained.

4. Results and Discussions

Firstly, we experimentally evaluate the position tracking performance, which is one of the key elements in the proposed dynamically secured MIMO VLC system. Figure 8 shows the experimental performance evaluation of the tracked moving receiver with different camera resolutions at various positions in the moving path using techniques discussed in Section 2. The practical results indicate that the average positioning error occurring between the original and the recorded scene for the lowest camera resolution (320×240) in a Cartesian coordinates system is (2.53 cm, 2.14 cm). Correspondingly, the measured standard deviation and maximum error values correspond to this under test resolution are (2.73, 1.87), (37.89, 7.92) respectively. For other higher camera resolutions, the corresponding system performance is summarised in Table 3.

Also, the minimum error value between the original and the recorded values with different resolutions is (0 cm). Note that though the resolutions are different, the errors seem to be converged and largely unvaried, the usage of the blob shape in the localisation of the moving receiver minimizes the positioning errors. This investigation indicates that we could use a low camera resolution for the proposed system, hence reducing the complexity, cost, and computational power requirement.

A further test is carried out to determine the effect of the outdoor ambient light intensity level (i.e., ambient noise) on the camera tracking system since the user might move/walk to different areas where the illumination levels are not the same. In this type of test, we experimentally measure the system performance in different ambient noise levels. The lux meter was placed at the receiver location (i.e., receiver plane) in order to estimate the real value of the ambient noise prior to initialising the tracking operation.

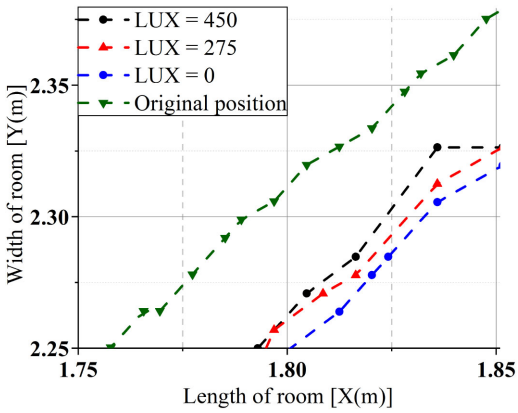
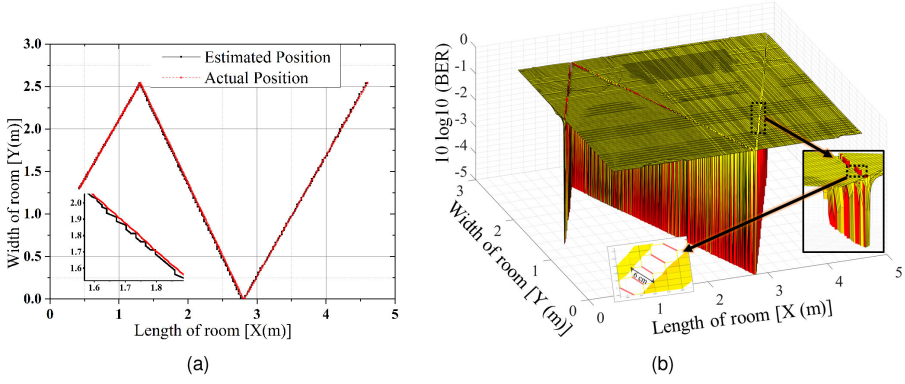


Fig. 9. The zoom-in effect of various ambient noise illumination levels at the receiver on the camera-based tracking performance with (distance = 2 m, and resolution = 1280 × 720).

TABLE 4
Tracking System Performance of Various Light Intensities

Illumination (Lux)	Error Mean X(cm),Y(cm)	Standard Deviation X(cm),Y(cm)	Maximum Error X(cm),Y(cm)
450	2.54, 1.37	1.26, 1.27	6.64, 6.66
275	3.72, 1.03	1.41, 0.99	6.64, 5.41
0	2.47, 1.46	1.33, 1.19	12.5, 5.41



(a) (b)

Fig. 10. (a) Comparison between the actual and estimated position for the entire room. (b) BER mapping for (resolution = 1280 × 720, distance = 2 m, and normal indoor light condition Lux = 450).

Different lighting levels will lead to a fluctuation of the camera's position detection performance. Low light circumstances will create a large noise in the acquired image [25], and that affects the accuracy of our proposed localisation scheme. Results illustrated in Fig. 9 as well as in Table 4 present the error of the positioning determined in the proposed tracking system with the ambient noise level of (450, 275, and 0 lux, i.e. standard lighting, dimming and dark conditions).

The lowest accuracy of the positioning system occurs when lux = 0 (i.e. no light at the receiver, where the background subtraction method in the camera does not perform well). In a dark condition, the observed x-axis maximum error is (12.5 cm) compared with (6.64 cm) error with normal indoor light conditions. Hence in a well-lit room, the tracking is much more reliable with regard to the camera's resolution.

Figure 10(a) presents a motion path of the authenticated receiver (user) inside the illuminated region. The motion path includes 160 tracked points. The transmitter sends a signal with a length

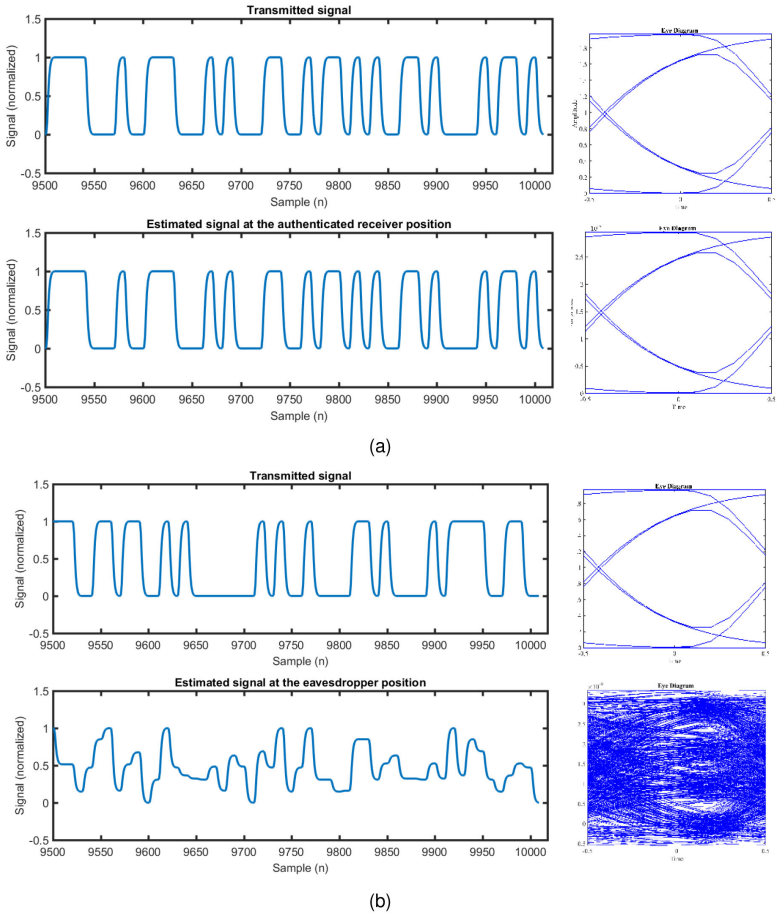


Fig. 11. The transmitted and estimated signals of an individual PD receiver for (a) The legitimate user. (b) The Eavesdropper.

of 1000 bits at each of the tracked points. The number of samples per bit is 10. The security performance of the system is measured by means of BER calculation at the receiver side, the BER obtained in Fig. 10(b) for the user when moving along the path is minimalized (BER $< 10^{-5}$) as the transmitter adaptively designs the secured communication channel to follow the motion path of the legitimate user. The beam-width of the secured communication zone is approximately 6 cm with respect to x and y coordinates which shows a very good physical security performance of the link. The transmitted and estimated signals by an individual PD at the legitimate user is showed in Fig. 11(a), whereas the recovered signal by an individual PD at the eavesdropper is depicted in Fig. 11(b). The successful demonstration has shown that the proposed dynamically secured MIMO VLC system operates properly when incorporating the position tracking approach under user movement scenarios.

Finally, we experimentally reconfigure the distance between the camera (in the transmitter side) and the user (in the receiver plane). The measurement results show that an average position error is (3.5 cm, 5.21 cm) for the distance h of 2 m and 3 m respectively as shown in Fig. 12.

The proposed algorithm can work properly with respect to these ranges, hence, low BER accuracy (at 10^{-5}) can be maintained within these ranges as depicted in Fig. 10(b). Note that, BER is estimated for different SNR conditions since Fig. 13 shows that the receiver in the communication zone is able to recover the transmitted data with SNR more than (40 dB) for the resolution of 1280×720, distance of 2 m, and normal indoor light condition of 450 Lux, whilst the eavesdropper in the non-communication zone is incapable of recovering the data.

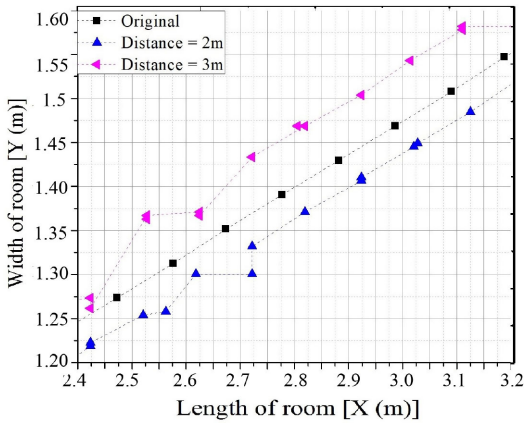


Fig. 12. The effect of different distance between the Camera-based surveillance system and the receiver plane for (resolution = 1280 × 720, distance = 2 m, and normal indoor light condition Lux = 450).

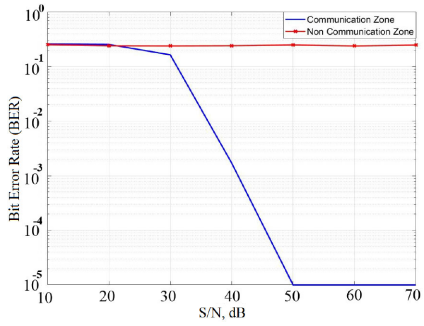


Fig. 13. BER against SNR for the MIMO VLC system for different position of receiver (inside and outside the communication zone) with (resolution = 1280 × 720, distance = 2 m, and normal indoor light condition Lux = 450).

The speed of detection varies according to the number of recorded frames, minimum blob area that been set, and the light condition in the room, however, the **P** matrix average estimated generation time based on MATLAB was 188 μs, whereas the standard deviation was 120 μs using Intel Core $i5-6200$ with 4 GB RAM (LENOVO - 80TY), therefore, the system can accommodate a real-time moving receiver. The system can be implemented using the integrated circuit design (i.e., field-programmable gate array (FPGA)) platform which could outperform the graphics processing unit (GPU) utilised in this study [5].

5. Conclusion and Future Works

The paper has introduced a new approach that integrates the computer vision into a MIMO VLC system, providing dynamic physical-layer security. The receiver location is demonstrated by using a camera-assisted system to dynamically assign a new secured communication zone. The test includes an investigation of transmitting and receiving signals of different locations in the illuminated area, exploring the receiver detection in the image-plane through background subtraction algorithm based on Gaussian mixture models, followed by tracking it within the video frames using blob analysis and mapping its position into the room-coordinates. Extensive tests and analysis were carried out for a moving receiver with a speed of 0.5 m/s (equivalent to a slow walk) under different scenarios to investigate the resolutions, light intensity level, and distance of used cameras. The proposed system offered suppression of eavesdroppers from gathering valuable information within the illuminated region. The data coverage width of the secured communication zone was

approximately 6 cm with respect to *x* and *y* coordinates. The BER mapping achieved in the results outlined a reasonable performance for a standard camera. In the future, the experimental work will be further extended to introduce machine learning to define different receivers based on visual and movement characteristics of the receiver without the need of a reference matrix. We will also consider the use of an imaging receiver to further improve the capacity of the system.

Acknowledgment

The authors would like to thank Hubert Dzieciol (University College London) and the anonymous reviewers for their comments to improve the quality of the paper.

References

[1] S. Dimitrov and H. Haas, *Principles LED Light Commun.: Towards Networked Li-Fi*. Cambridge, U.K.: Cambridge Univ. Press, 2015.
[2] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Opt. Wireless Commun.: System and Channel Modelling With Matlab*. Boca Raton, FL, USA: CRC press, 2012.
[3] A. H. Azhar, T. Tran, and D. O'Brien, "A gigabit/s indoor wireless transmission using mimo-ofdm visible-light communications," *IEEE Photon. Technol. Lett.*, vol. 25, no. 2, pp. 171–174, Jan. 2013.
[4] Z. Zhen *et al.*, "1.2 gbps non-imaging mimo-ofdm scheme based vlc over indoor lighting led arrangments," in *Proc. Opto-Electron. Commun. Conf.*, 2015, pp. 1–3.
[5] F. Wu, C. Lin, C. Wei, C. Chen, H. Huang, and C. Ho, "1.1-gb/s white-led-based visible light communication employing carrier-less amplitude and phase modulation," *IEEE Photon. Technol. Lett.*, vol. 24, no. 19, pp. 1730–1732, Oct. 2012.
[6] Z. Che, J. Fang, Z. L. Jiang, X. Yu, G. Xi, and Z. Chen, "A physical-layer secure coding schcme for visible light communication based on polar codes," in *Proc. Conf. Lasers Electro-Opt. Pacific Rim*, 2017, pp. 1–2.
[7] A. Mukherjee, S. Ali A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Jul.–Sep. 2014.
[8] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in *Proc. Globecom Workshops*, 2014, pp. 505–511.
[9] A. Mostafa and L. Lampe., "Physical-layer security for miso visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.
[10] H. Lu, L. Zhang, W. Chen, and Z. Wu, "Design and analysis of physical layer security based on ill-posed theory for optical ofdm-based vlc system over real-valued visible light channel" *IEEE Photon. J.*, vol. 8, no. 6, pp. 1–19, Dec. 2016.
[11] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–14, Oct. 2016.
[12] Z. Che, J. Fang, Z. L. Jiang, J. Li, S. Zhao, Y. Zhong, and Z. Chen, "A Physical-Layer Secure Coding Scheme for Indoor Visible Light Communication Based on Polar Codes," *IEEE Photon. J.*, vol. 10, no. 5, pp. 1–13, Oct. 2018.
[13] S. Shao *et al.*, "An indoor hybrid wifi-vlc internet access system," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, 2014, pp. 569–574.
[14] O. I. Younus, N. Bani Hassan, Z. Ghassemlooy, P. A. Haigh, S. Zvanovec, L. N. Alves, and H. L. Minh, "Data Rate Enhancement in Optical Camera Communications Using an Artificial Neural Network Equaliser," In *IEEE Access*, vol. 8, pp. 42656–42665, 2020.
[15] P. Djahani and J. Kahn, "Analysis of infrared wireless links employing multibeam transmitters and imaging diversity receivers," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2077–2088, Dec. 2000.
[16] S. Rajbhandari, "Spatial and wavelength division multiplexing for high-speed VLC systems: An overview" in *Proc. 10th Int. Symp. Commun. Syst., Netw. Digit. Signal Process.*, 2016, pp. 1–6.
[17] F. I. K. Mousa, N. Al Maadeed, K. Busawon, A. Bouridane, and R. Binns, "Secure mimo visible light communication system based on users location and encryption," *J. Lightw. Technol.*, vol. 35 no. 24, pp. 5324–5334, 2017.
[18] M. Piccardi, "Background subtraction techniques: A review," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, 2004, vol. 4, pp. 3099–3104.
[19] P. W. Power and J. A. Schoonees, "Understanding background mixture models for foreground segmentation," in *Proc. Image Vision Comput.*, New Zealand, vol. 2002, 2002, pp. 10–11.
[20] S. C. Sen-Ching and C. Kamath, "Robust techniques for background subtraction in urban traffic video," in *Proc. Visual Commun. Image Process.*, International Society for Optics and Photonics, vol. 5308, 2004, pp. 881–892.
[21] C. Stauffer and W. E. L. Grimson, "Adaptive background mixture models for real-time tracking," in *Proc. IEEE Comput. Soc. Conf. Comput. Vision Pattern Recognit.*, 1999, vol. 2, pp. 246–252.
[22] A. Chantakamo and M. Ketcham, "The multi vehicle recognition using hybrid blob analysis and feature-based," in *Proc. 7th Int. Conf. Inform. Technol. Elect. Eng.*, 2015, pp. 453–457.
[23] H. Zhou, L. Llewellyn, L. Wei, D. Creighton, and S. Nahavandi, "Marine object detection using background modelling and blob analysis," in *Proc. IEEE Int. Conf. Syst., Man, and Cybern.*, 2015, pp. 430–435.
[24] W. D. Pence, L. Chiappetti, C. G. Page, R. A. Shaw, and E. Stobie, "Definition of the flexible image transport system (fits), version 3.0," *A A*, vol. 524, pp. 73–75, 2010.
[25] Huaxin Xiao, Yu Liu, Shuren Tan, Jiang Duan, and Maojun Zhang, "A noisy videos background subtraction algorithm based on dictionary learning," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 6, pp. 1946–1963, 2014.